JUL 26 2004

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	22.Jul.04	MAJOR REPORT

4. TITLE AND SUBTITLE
CYBER WARFARE: RAISING INFORMATION SECURITY TO A TOP PRIORITY

5. FUNDING NUMBERS

6. AUTHOR(S)
MAJ KNAPP KENNETH J

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
AUBURN UNIVERSITY MAIN CAMPUS

8. PERFORMING ORGANIZATION REPORT NUMBER
CI04-492

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
THE DEPARTMENT OF THE AIR FORCE
AFIT/CIA, BLDG 125
2950 P STREET
WPAFB OH 45433

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION AVAILABILITY STATEMENT
Unlimited distribution
In Accordance With AFI 35-205/AFIT Sup 1

12b. DISTRIBUTION CODE

13. ABSTRACT *(Maximum 200 words)*

DISTRIBUTION STATEMENT A
Approved for Public Release
Distribution Unlimited

20040809 066

14. SUBJECT TERMS	15. NUMBER OF PAGES
	32
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT

Cyber Warfare:

Raising information security to a top priority.

Kenneth J. Knapp

Doctoral Candidate

College of Business

Auburn University

knappkj@auburn.edu

William R. Boulton

C.G. Mills Professor of Strategic Management

College of Business

Auburn University

boulton@business.auburn.edu

ABSTRACT

Beyond the media hype, information warfare has become a central concern of the Internet age. While not denying the obvious military implications, a 15-year review (1990-2004) of information conflict reveals twelve characteristics and trends that affect civilian communities as well. For example, there is the growing availability of low-cost cyber weaponry on the Internet as modern societies increasingly rely on information infrastructures, and civilian organizations become the primary targets of attacks. Additionally, information warfare encompasses such domains as espionage, media perception, nation-state relations, and transnational criminal activities. As information conflict becomes a growing concern, managers must understand this reality and plan to defend against attacks. As a conclusion, this article provides a summary of the twelve selected characteristics of information conflict and offers a comprehensive strategy to promote effective information security in organizations.

THE VIEWS EXPRESSED IN THIS ARTICLE ARE THOSE OF THE AUTHOR AND DO NOT REFLECT THE OFFICIAL POLICY OR POSITION OF THE UNITED STATES AIR FORCE, DEPARTMENT OF DEFENSE, OR THE U.S. GOVERNMENT.

Introduction

Commonly considered a military concern, information warfare has become a broader society issue. While information warfare has suffered from its share of media hype, increased conflict over the Internet has raised information security to be a dominant concern of business managers.[1] While the bulk of the literature and attention addresses the military community, information warfare has become a civilian concern.[2-4] While not denying the obvious military implications, a 15-year review (1990-2004) reveals twelve characteristics and trends that suggest that information warfare has predominantly become a civilian form of conflict. This shift presents a growing threat to information managers who are responsible for protecting their organizations' information assets.

A number of important characteristics and trends lead to this conclusion. Among these trends include the alarming availability of low-cost information weaponry through the Internet, the targeting of civilian information assets, and the growing economic dependency of modern societies on information infrastructures.[5] Additionally, we have seen a mounting number of attacks through the Internet. After monitoring hundreds of the Fortune 1000 companies, Bagchi & Udo recorded an annual 64% growth rate in cyber attacks.[6] As Table 1 shows, based on selected indicators, the growth rate of these incidents has outpaced Internet growth since 1998. This pattern indicates an ever-increasing level of conflict over the Internet. The conventional militaries lack both the resources and responsibility to defend their governments' national infrastructures from such attacks.[7] Managers must understand this reality and plan to defend against threats. The intent of this paper is to identify and describe the trends and

characteristics that best illustrate the intensity of conflict arising through the Internet. As a conclusion, this article provides a summary of the twelve selected characteristics of information conflict and offers a comprehensive strategy to respond to this threat through effective information security in organizations.

TABLE 1. Growth in the Internet versus reported security incidents[8]

Average annual Internet growth 1990-1996	132%	Average annual growth in reported incidents 1990-1997	48%
Average annual Internet growth 1997-2002	47%	Average annual growth in reported incidents 1998-2002	112%

Defining Information Warfare and its Context

Webster's New World Dictionary defines *conflict* as 1) a fight or war and 2) a sharp disagreement, and defines *warfare* as 1) the action of waging war; armed conflict and 2) as a conflict or struggle of any kind. For this paper, we use *conflict* and *warfare* interchangeable. We explore a range of information conflict types, covering political, economic, criminal, security, and military dimensions.

The term *information warfare* reportedly originated in 1976 from the late MIT professor, Dr. Thomas Rona. Since then, proposed definitions have emphasized both military and civilian contexts. Testifying before Congress in 1991, Winn Schwartau stated that poorly protected government and commercial computer systems were vulnerable to an "electronic Pearl Harbor".[9] Most definitions originated from the military community. Libicki offered seven categories of information warfare replete with military terminology: command and control warfare, intelligence-base warfare, electronic warfare, psychological warfare, hacker warfare, economic information warfare, and cyberwarfare.[10]

Some authors have developed context neutral definitions. Cronin & Crawford argued that information warfare concepts need liberation from military associations and introduction to communities that understand the consequences of pervasive computing in society.[3] They consider four spheres where information warfare may become commonplace: military, corporate-economic, community-social, and personal. Cronin defines information warfare as those actions intended to protect, exploit, corrupt, deny, or destroy information or information resources in order to achieve a significant advantage, objective or victory over an adversary.[11] This comprehensive definition

comprises military, economic, societal, personal, and the security dimensions of information warfare.

The *National Strategy to Secure Cyberspace*[5] lists a five-level security problem, detailed in Table 2. These five levels include individual home and small business users. The report is concerned that undefended home and small business computers, particularly those using digital subscriber lines (DSL) or cable connections, will unsuspectingly support denial-of-service attacks directed at key Internet nodes and other important enterprises or critical infrastructure. Scholars share the concern that an enemy of the United States will launch an information warfare attack against civilian and commercial firms and infrastructures.[12]

TABLE 2. Five-level problem in cyberspace

Level 1	Home users, small businesses, private individuals
Level 2	Large enterprises, corporations
Level 3	Critical sectors, infrastructures
Level 4	National issues and vulnerabilities, national-level problems
Level 5	Global, planetary information grid of systems

Significant Characteristics and Trends of Information Warfare

Security incidents are widespread and underreported

Two highly referenced information security measures come from the CERT/CC[13] and the annual CSI/FBI survey.[14] Figure 1 illustrates the growing number of incidents reported to the CERT/CC over the past fifteen years. Note the explosive rise since 1998. Table 3 offers a year-by-year comparison of the data introduced in Table 1. It compares CERT/CC incident data with Internet Software Consortium[15] host growth data. Based on these metrics, since 1998, the growth in reported incidents to the CERT/CC has outpaced the growth in hosts connected to the Internet. Without researching the reason behind these data, the figures suggest a rising trend in incidents.

FIGURE 1. Incidents reported to CERT/CC, 1988-2003

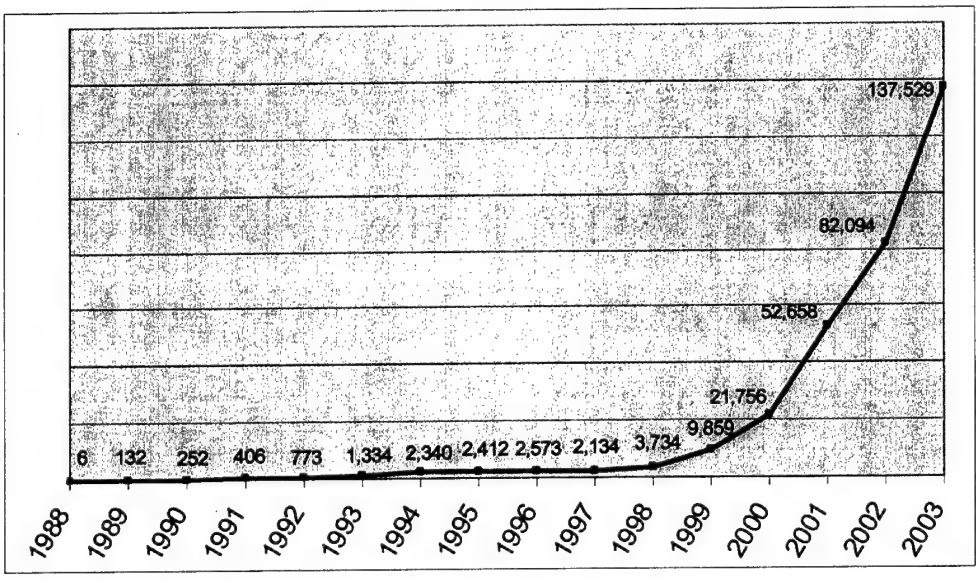

TABLE 3. Reported incidents and Internet host growth between years 1993-2002.

Year (A)	CERT/CC reported incidents (B)	Increase from previous year (C)	ISC reported Internet hosts (D)	Increase from previous year (E)	Column (C) – (E)
1993	1,334	73%	1,776,000	79%	(6%)
1994	2,340	75%	3,212,000	81%	(6%)
1995	2,412	3%	8,200,000	155%	(152%)
1996	2,573	7%	16,729,000	104%	(97%)
1997	2,134	(17%)	26,053,000	56%	(73%)
1998	3,734	75%	36,739,000	41%	34%
1999	9,859	164%	56,218,000	53%	111%
2000	21,756	121%	93,047,785	66%	55%
2001	52,658	142%	125,888,197	35%	107%
2002	82,094	56%	162,128,493	29%	27%

Since its inception in 1996, the annual CSI/FBI survey has closely measured computer crime trends to develop a sense of the 'facts on the ground.' The survey reports more illegal and unauthorized cyberspace activities than corporations admit to their clients, stockholders and business partners or report to law enforcement. These incidents are widespread, costly and commonplace. Further, the survey challenges the profession's conventional wisdom that these threats come from inside the organization. Survey results show a greater threat from outside the organization. Based on the 2002 report, ninety percent of respondents, primarily large corporations and government agencies, had detected computer security breaches within the last twelve months. Only thirty-four percent reported such intrusions to law enforcement agencies.[16]

We can draw three conclusions from these statistics. First, information security incidents are prevalent and have increased over the years. Second, civilian institutions are the target of a large number of these attacks. Third, many of these incidents are not publicly acknowledged.

Technical and financial entry barriers are low for cyber attackers

Early generations of cyber weaponry (i.e. hacker tools) required knowledge of how computer operating systems and TCP/IP worked. For instance, hackers of the 1960s often emerged from MIT.[17] Robert Morris, Jr., a graduate student at Cornell University and son of a chief scientist at the National Security Agency, developed the 1988 Internet worm that affected 6,200 computers costing an estimated 100 million dollars in cleanup (Zviran, 1999).[18] Compare this to the teenage-hacker typified by the main character in the popular 1983 movie *War Games*. While this teenager stereotype may hold some truth, much of the early hacking actually required advanced skills.

The hacker environment began changing in the early 1990s as technical barriers began to fall as downloadable and graphic-interfaced tools became widely available.[19] A notorious incident involving teenagers occurred in the late 1990s. In a series of events labeled Solar Sunrise, two teenage hackers, under the guidance of an eighteen-year old Israeli mentor, gained access to computers at eleven U.S. Air Force and Naval bases.[20] Solar Sunrise served as a warning that serious hacking capabilities are within the grasp of relative non-experts.

Testifying before Congress in 1999, CIA Director George Tenent stated that, terrorists and others are recognizing that information warfare offers them low cost, and easily hidden tools with which to support their causes. Many of these tools are windows-based, require minimal technical understanding, and are often available as freeware. One IS security professional maintains a database of over 6,000 hacker sites believed to contain only a part of the better hacker tools.[20]

Today, networked organizations employ sophisticated defensive devices such as firewalls, intrusion detection systems, and proxy servers.[21] Penetrating a robust, properly configured network defense can require advanced computer skills. Unfortunately, many network devices are either improperly configured or have known vulnerabilities, leaving significant opportunities for low skilled hackers using pre-packaged tools. Additionally, intruders often cleverly dupe employees into giving away information, such as important passwords, and then hack into the heart of corporate networks.[22] Since engaging in cyber attacks does not require an attacker to have substantial resources, organizations must be vigilant and employ strong and properly configured defenses against these dangerous threats.

Organizational barriers against strategic cyber attack are higher

Strategic warfare occurs when attackers use weapons against infrastructures and centers of gravity.[23] Strategic targets include high value military or commercial operations. Because high-value cyber targets have stronger defenses, attacks require considerable technical and financial resources, as well as organizational resources. Competent leadership, planning, recruiting and training become necessary organizational ingredients in order to successfully plan and implement strategic attacks.

Strategic information warfare actors must seek competitive advantages if they are to achieve their goals. Sufficient levels of information technology innovation, adoption, diffusion, and assimilation in the organization is required.[23] The same levels of organizational effectiveness seen in the business world may be required for a successful strategic information attack. Since these capabilities require resources and longer-term commitment, we should expect that strategic information warfare capabilities would require some type of financial sponsorship, such as from a nation-state or a commercial or criminal enterprise. This expectation suggests that one's ability to engage in strategic cyber attacks will be more difficult than for non-strategic attacks.

Nations have developed information warfare tools

In the early 1990s, few nations had an organized information warfare capability. Some sources now believe that more than 30 nations have developed organized, computer-based information warfare programs, including Russia, China, Taiwan, Iran, Israel, France, India and Brazil[24]. In the 2003 CSI/FBI survey, 28% of respondents identified foreign governments as a likely source of attack against their systems.

Cyber Warfare: Raising information security to a top priority.

China provides an interesting case of a nation that is building information warfare capabilities. According to Chinese Major General Wang Pufeng in 1995:

> "In the near feature, information warfare will control the form and future of war. We recognize this developmental trend of information warfare and see it as a driving force in the modernization of China's military and combat readiness. This trend will be highly critical to achieving victory in future wars".[20]

To further advance China's capabilities, new research institutes are focusing on asymmetric and non-traditional warfare strategies. These institutes employ thousands of researchers investigating ways to exploit weak spots in technologically superior foes using computer attacks, electronic interference and other information warfare techniques.[25] This may be potentially threatening when considering that Chinese "hackivists" have attacked U.S. Internet sites in the past.[26] Others are concerned of an information war across the Taiwan Strait.[27]

While the U.S. military is concerned with state-sponsored information warfare programs, commercial businesses must pay attention as well. With a suspected 30 countries actively pursuing information warfare weaponry, business and government executives alike must assess their vulnerabilities from a concerted cyber attack. This line of thinking extends Drucker's admonishment of executives to look outside their organizations for business opportunities and information.[28] Likewise, executives should seriously look outside their organizations for cyber threats as well.

Economic dependency on the information infrastructure and technology

The evolution from an agrarian to an industrial to an information-based society has received significant discussion. References to the "digital economy" and "third wave"[29] describe our growing dependence on information technology. With a growing concern about potential disruptions,[30] the U.S. Government seriously addressed the deepening economic dependency on computers in the National Research Council's 1991 report, *Computers at Risk*. This report expressed concern that computers "control power delivery, communications, aviation, and financial services. They are used to store vital information, from medical records to business plans to criminal records".[23] But it wasn't until 1998 that the National Infrastructure Protection Center (NIPC) was established. In 2003, NIPC merged into the Department of Homeland Security to help protect these critical infrastructures.

With an increasing reliance on information technology, there is a growing need to protect it. In 1998, Presidential Directive (PDD) 63 designated federal agencies to initiate development of protective measures for specified infrastructures. Table 4 shows the responsibilities of key agencies. In cooperation with the private-sector, each agency is developing an Information Sharing and Analysis Center (ISAC) to identify existing and emerging vulnerabilities. Private sector owners establish each ISAC to gather, analyze, and disseminate information about the threats and vulnerabilities faced by that sector. The first ISAC was established in the banking and finance sector in October 1999. By 2004, over a dozen centers had been established.[31]

TABLE 4. Some federal agencies and assigned sectors.

Lead Federal Agency	Designated Infrastructure Sector
Environment Protection Agency	Water Supply
Department of Treasury	Banking and Finance sectors
Department of Energy	Power, Oil, Gas Production
Department of Commerce	Information and Communications
Department of Transportation	Aviation, highways, mass transit, pipelines, rail, waterborne commerce
Department of Justice/FBI	Emergency law enforcement

The 2003 *National Strategy to Secure Cyberspace* report set strategic objectives to prevent cyber attacks against critical infrastructures, to reduce national vulnerability to cyber attacks, and to minimize damage and recovery time from cyber attacks that do occur. The report recognized that,

> "By 2003, our economy and national security became fully dependent upon IT and the information infrastructure. A network of networks directly supports the operation of all sectors of our economy—energy, transportation, finance and banking, information and telecommunications, public health, emergency services, water, medical, defense industrial base, food, agriculture, and postal and shipping."[5]

While this report promotes government-industry cooperation, it notes that the private sector was better equipped and structured to respond to the evolving cyber threat. Areas that would benefit from government-industry cooperation include the sharing of defensive strategies and tactics. For example, *defense in depth* has been an element of U.S. Nuclear Commission's safety philosophy that employs successive and redundant measures to prevent accidents at nuclear facilities. This philosophy has served the nuclear power industry well[32] and it provides an effective architectural model for securing industry cyber defenses.

New cyber-weapons are emerging

The first electronic message boards for hackers appeared around 1980; enabling hackers to exchange tactics and tools. Once available, these boards allowed the rapid sharing of software, including distributed denial-of-service (DDOS) tools. This software

was responsible for the February 7, 2000 attack which effectively shut down major Internet sites such as Yahoo, eBay, Amazon, E*Trade, and CNN.

With increasingly sophisticated technologies, smaller, cheaper, and more dangerous devices will create new technological threats. Over the past twenty years, many cyber weapons have become affordable and available to those seeking to use them, including spyware such as keystroke and eavesdropping devices. There are also high-energy radio frequency (HERF) and electromagnetic pulse (EMP) tools. *E-bombs*, designed to fry computer electronics with electromagnetic energy, can be built for as little as $400.[33] These devices were demonstrated in 1994. According to a London Sunday Times report, the Defense Research Agency believed HERF guns initially blacked out computers used by London's financial houses. Cyberterrorists reportedly then extorted millions of pounds by threatening to totally knock out these financial computer systems.[34]

Private sectors have become primary targets

Many high profile information attacks initially targeted the military. The 1986 *Cuckoo's Egg* incident had Clifford Stoll tracking German hackers who were scouring American military systems.[35] During the 1994 Griffis Air Force Base incident, hackers used computers to launch attacks at other military, civilian, and government organizations. Seeking to avoid a direct military confrontation with U.S. forces, foreign aggressors are shifting their attacks to the "soft American underbelly," the private sector, in a way that can make military retaliation very difficult.[24]

With the growing economic dependency on IT infrastructures, it is likely that civilian infrastructures will increasingly become the primary targets of attacks. Recent

headline-grabbing cyber attacks have targeted widely used software products and commercial web sites. Example attacks from 2003-2004 included SQL Slammer, MyDoom, and Sasser. The private and public sectors together now form the front line of twenty-first-century warfare, and private citizens are likely to be the first target.[24]

Increasing technology use in perception management

Perception management reflects a view that image is the basis of reality. Examples of perception management cross the spectrum of corporate, political, civilian, and military realms. Perception management can include psychological operations, corporate marketing campaigns or state-sponsored propaganda activities. Fortune 500 companies take notice when web sites critical of their company appear highly ranked on popular search engine results.[36]

What distinguishes modern perception management from traditional propaganda is the role of information technology in influencing the formation of public perception and opinion. The information age has introduced new tools for practicing perception management, increasing the speed of media reporting and intrusiveness. The rise of global television and Internet technologies makes perception management a crucial dimension for all types of conflicts.[23] The Chinese government has made extensive use of perception management tools.[37] The Somalis, Haitians, and Bosnian Serbs successfully used global television as a political instrument to reverse U.S. policy decisions.[38]

Perception wars target the courts of public opinion. Consider the numerous electronic perception battles in the 2003-2004 Iraqi War. In 2003, anti-war activists used the Internet to organize and promote marches and rallies. Embedded wartime

reporters traveling with military units provided favorable news coverage for the campaign. In contrast, the Qatar-based news agency Al-Jazeera transmitted images of dead and wounded Iraqi civilians to the Arab world. Al-Jazeera also launched an English web site in part to counter what some believed to be U.S. military censorship of the American-based media. The Al-Jazeera web site itself was then hacked and taken off line. In 2004, electronic imagines of abuse at Abu Ghraib prison shocked the world, influencing public opinion regarding American conduct and values.

Information technology and corporate espionage

While espionage activity has been used for thousands of years, increased global competition and advances in IT, especially with the increased availability of tiny, embedded devices, have added considerably to espionage dangers. Some security analysts note that the French government has engaged in significant high technology espionage, claiming that French authorities have placed hidden copying devices in paper shredders conveniently available in French hotels frequented by foreign business travelers.[20] In March 2001, former Defense Secretary William Cohen identified the former director of French intelligence as publicly admitting that French intelligence secretly collects and forwards to French companies information about their competitors in the United States and elsewhere. Cohen described the implications for the business community of this proliferation of embedded networked devices. He gave three specific examples of French espionage against American companies. While the average cost of a hacking attack or denial of service is roughly $150,000 to a company, according to the FBI, the average loss of a corporate espionage incident is much larger.[39]

Espionage can occur in email communications between employees of business competitors. Market research firm NFO InDepth Interactive surveyed 498 employees in a variety of organizations. Forty percent of those surveyed admitted to receiving confidential information about other companies via the Internet, a 356% increase since 1999.[40] As organizations open their internal networks and make more company information available to employees and vendors, the opportunities for and occurrence of corporate espionage will likely mount.

Organized cyber-crime is an international problem

With the explosion of Internet usage come newer forms and levels of cyber crime. In May 2003, the Department of Justice announced a national operation, dubbed Operation E-Con, to root out some leading forms of online economic crime.[41] The Department claims that Internet fraud and other forms of online economic crime are among the fastest growing crimes. One of these crimes is web site scams. For example, Australian scammers targeted Bank of America customers by implementing a look-alike Website. Customers where sent scammed emails that directed them to the fake site which acquired their account names and passwords upon logging onto the site. These criminals compromised approximately 70 customer accounts.

Nigerian cyber gangs are notorious for "419" or advance-fee scams which used dozens of fake bank web sites operated out of Amsterdam to provide credibility that could not have been developed in Nigeria.[42] As shown by the annual CSI/FBI surveys, cyber-crime continues to proliferate. The Millennium Project, a futurist group associated with the American Council at the United Nations University, has called for a "declaration

of information warfare" against transnational organized crime to encourage businesses and nations to take this problem more seriously.[43]

Cyber-insurance demand is growing

Considering the importance of information resources to organizations and societies, the growing threat to those resources is raising the need for risk mitigation strategies such as cyber-insurance. While cyber intrusions often goes unreported to avoid negative publicity, at least two dozen insurance companies offered cyber policies by 2002, including such firms as Chubb, Lloyd's of London, Zurich North America, and American International Group. Cyber-insurance policies have higher premiums and deductibles because of the uncertainties in assessing cyber-risk.[44] USA Today reported that the average cost for cyber-insurance ranges from $5,000 to $30,000 per year for $1 million in coverage.

After only three years in the market, network risk insurance or "hacker insurance" reached about $100 million in 2002. It is expected to reach $2.5 billion by 2005, according to insurance industry projections.[45] The U. S. President's National Strategy to Secure Cyberspace report recommends insurance "as a means of transferring risk and providing for business continuity".[5] The 2001 Code Red Worm incident cost its victims and insurance companies an estimated $2 billion in damage. Computer Economics estimates that damages caused by The Love Bug, Melissa, Code Red and other vulnerabilities exceeded $54 billion in down time, removal expenses and repairs.[46] A survey of 500 U.S. companies showed an increase in reported financial losses of *21 percent*, or $455.8 million in 2002. In addition, those losses are increasingly the result of organized, planned cyberattacks.[16] According to an Ernst and Young survey,

security occurrences can cost companies between $17 and $28 million per incident.[47] By 2005, there will be 400 million Internet-connected computers worldwide, two billion Internet-enabled mobile devices and one billion users of Internet messaging. This means that companies will have a host of new security concerns.[48] As cyber-related incidents like this continue, demand for insurance to cover such losses as well as electronic theft, vandalism, and extortion will likely grow.

The growing information security profession

For years, systems security took a back-burner amongst information technology executives.[49] With the changing threat environment, however, security is moving to the front. New specialists are now in demand to help organizations protect their information resources. Certified professionals act as organizational leaders in security. They help senior management in the important roles of security education, training, and awareness, risk assessment, and the promotion of a security-minded culture.[50] The dramatic growth in the number of Certified Information Systems Security Professionals (CISSP) attests to this need. This certification program has grown from 2,000 total certifications in 1999 to over 25,000 in 2004.[51] Additionally, curricula in information security & assurance are appearing throughout academia. The 2004 $(ISC)^2$ Resource Guide lists numerous institutes of higher learning that now offer various types of information security programs.

Conclusion

A body of evidence suggests that the types and intensity of high-tech information warfare and attacks are increasing. Table 5 summarizes the twelve important

characteristics and measures discussed in this paper, supporting the thesis that information warfare is of growing importance and concern. Spurred by growth of the global Internet, an increasing number of non-military individuals, enterprises and commercial infrastructures are targets for cyber attackers. As the bulk of information warfare conflict moves into a civilian-dominated context, the cost to commercial organizations has reached tens of billions of dollars. These costs can no longer be ignored and require that security become a top priority for industry and society.

TABLE 5. Characteristics of information conflict, 1990-2004

Information Conflict Characteristics and Measures	1990 (unless noted)	2004
CERT/CC Reported Incidents	252	137,529 (2003)
Technical and Financial Entry Barriers to engage in cyber attacks	Significant	Insignificant
Organizational Barriers for Strategic Information Warfare	Not applicable	High
Countries with Information Warfare Programs	Few	30+
Economic Dependency on Information Infrastructures	Partial	Full
Forms of Cyber Weapons	Fewer, lower availability	Many types available & affordable
Primary Targets in Information Conflicts	Military and Civilian	Increasingly Civilian
Use of Technology in Perception Management	Global TV, radio	Global Multi-media
Corporate Cyber Espionage	Growing	Substantial
International Organized Cyber Crime	Growing	Substantial
Corporate Cyber Insurance	Few offerings	20+ companies
Information Security Professionals (CISSP)	2,000 (1999)	Over 25,000 (2004)

Cyber Warfare: Raising information security to a top priority.

Historically, information security concerns have not had a high priority with most managers. Many managers seemed willing to risk major losses by permitting their information systems to be either lightly protected or wholly unprotected.[52] Yet, our growing reliance on information technologies and the Internet has increased our exposure to diverse sources of cyber attacks. Corporate leaders must be aware of the diversity of attacks, including high-tech espionage, crime, perception battles, hackers, and attacks from groups sponsored by nation-states or business competitors. Senior managers can no longer afford to put their information resources and infrastructures at risk. Top management's awareness and commitment is required to address this problem.[50] Security complacency has increased the risks for many organizations, especially for those whose programs that appear effective and have not suffered from direct attacks. Nevertheless, considering the full range of cyber threats facing commercial organizations today, management must ensure that security is a top priority. With the average cost of an incident ranging from $17 million to $28 million, firms can afford to support the implementation of a cyber security strategy.

Implication for managers: Implement a Comprehensive Cyber Security Strategy

The trends identified in Table 5 show the diversity of threats and the need for vigilance and management attention. Thus, to ensure effective security in their organizations, managers need to develop two critical strategies: an architectural strategy and a managerial strategy. First, a protection strategy includes layers of protection in order to increase the time and resources necessary by attackers to penetrate the multiple levels of security barriers. This *defense in depth* strategy is similar to an architectural fortress of high walls and armed guards behind a protective

moat.[53] While each barrier alone does not ensure sufficient protection, taken together, a layering of firewalls, with anti-virus software, and intrusion detection systems, can greatly help an organization defend itself from the many types of attacks mentioned in this paper.

While *defense in depth* is an excellent strategy to help protect against cyber threats, many of today's security problems require managerial rather than technical solutions.[54] A managerial strategy should flow from the thesis of this paper and include four principal components: hiring certified security officers, training employees, assessing risk, and managing policy. The first step is to hire certified security professionals as the commissioned officers of the Cyberwar. These security officers must be leaders with appropriate authority in the organization. With this authority, they can implement the second step of the strategy: the effective training and motivating of the foot soldiers in the Cyberwar. Since every employee is part of the security team, an untrained employee is a high-risk asset.[22] Security trained employees should understand that cyber threats come from not just the stereotypical hacker, but from business competitors, foreign governments, and organized crime.

The third part of the managerial strategy is to mandate annual risk assessments to identify cyber threats. With this, managers need to identify which threats are most risky and could cause the most damage, and spend the money needed to address the high priority threats.[55] The purchasing of cyber insurance is one risk mitigation strategy that can protect businesses from cyber disasters. However, most risks are mitigated by developing and enforcing a solid security policy, the fourth component in the

management strategy. Policies are the primary building blocks of every information security effort by providing managerial direction and support.[56] Yet, the best policies and training programs will be wasted efforts if employees disregard security policy. Effective enforcement of enterprise security policies through monitoring and automated auditing can reduce security risks.[5, 49] Clearly written security policies and their enforcement will promote good security and discipline in the organization. A *defense in depth* architecture strategy supported by a management strategy to hire, train, assess risks, and set policies can significantly help organizations defend themselves against the growing threat posed by today's high-tech information warfare. The absence of such strategies can only lead to a growing risk that organizations will eventually be hit by a major information attack and bare the multi-million dollar cost that result. We hope this paper will help initiate the appropriate strategies needed to mitigate such a threat.

References

1. Porter, Tim. "Information Warfare - Your Company Needs You!" *Computers & Security* 15 (1996): 561-66.
2. Cronin, Blaise. "Information Warfare." *Library Journal* 127, no. 12 (2002): p54.
3. Cronin, Blaise, and Holly Crawford. "Information Warfare: Its Applications in Military and Civilian Contexts." *Information Society* 15, no. 4 (1999): 257-64.
4. Hutchinson, W. "Concepts in Information Warfare." *Logistics Information Management* 15, no. 5/6 (2002): 410-13.
5. President. *National Strategy to Secure Cyberspace [Rec.1-4(b)]* February, 2003. Accessed from http://www.whitehouse.gov/pcipb.
6. Bagchi, K., and Udo G. "An Analysis of the Growth of Computer and Internet Security Breaches." *Communications of the Association for Information Systems* 12, no. 46 (2003): 1-29.
7. Dearth, Douglas H. "Imperatives of Information Operations and Information Warfare." In *Cyberwar 2.0: Myths, Mysteries, and Reality*, edited by A.D. Campen and D.H. Dearth. Fairfax, VA: AFCEA International Press, 1998.
8. Data sources: www.isc.org and www.cert.org.
9. Schwartau, Winn. "Something Other Than War." In *Cyberwar 2.0: Myths, Mysteries, and Reality*, edited by A.D. Campen and D.H. Dearth. Fairfax, VA: AFCEA International Press., 1998.
10. Libicki, Martin C. *What is Information Warfare?* Washington, DC: National Defense University, Institute for National Strategic Studies, 1995.
11. Alger, J. I. "Introduction." In *Information warfare: Cyberterrorism: Protecting Your Personal Security in the Information Age*, edited by W Schwartau, 8-14. New York: Thunder's Mouth Press, 1996.
12. Strassmann, Paul A. *Government Should Blaze Global Information Warfare Trails*, 2001 [cited June 22, 2004]. Accessed from http://www.strassmann.com/pubs/searchsecurity/2001-8.php.
13. The Computer Emergency Response Team Coordination Center (CERT/CC) is operated by the Software Engineering Institute at Carnegie-Mellon University.
14. The Computer Crime and Security Survey is annually conducted by the Computer Security Institute with the participation by the San Francisco Federal Bureau of Investigation's (FBI) Computer Intrusion Squad.
15. Number of Hosts as reported by the Internet Software Consortium (www.isc.org). Figures represent each year's July measure.
16. Computer Security Institute. "Eight Annual, 2003 CSI/FBI Computer Crime and Security Survey." 22p: CSI, 2003.
17. PCWorld. *Timeline: A 40-year history of hacking* IDG News Service, November 19, 2001 [cited June 12, 2003]. Accessed from http://www.cnn.com/2001/TECH/internet/11/19/hack.history.idg/.
18. Zviran, Moshe, and William J. Haga. "Password Security: An Empirical Study." *Journal of Management Information Systems* 15, no. 4 (1999): 161-85.
19. A list of 75 security tools is provided at http://www.insecure.org/tools.html. This list is derived in part from a hacker mailing list. Many of the listed tools are free hacker tools that have been around for years.

20. Jones, A., Kovacich G.L., and Luzwick P.G. *Global Information Warfare: How Businesses, Governments, and Others Achieve Objectives and Attain Competitive Advantages*. New York: Auerbach Publications, 2002.
21. Sequeira, D. "Intrusion Protection Systems: Security's Silver Bullet?" *Business Communication Review* March (2003): 36-41.
22. Mitnick, Kevin. "Are You the Weak Link?" *Harvard Business Review* 81, no. 4, (2003): 18-20.
23. Rattray, Gregory J. *Strategic Warfare in Cyberspace*. Cambridge, MA: MIT Press, 2001.
24. Adams, J. "Virtual Defense." *Foreign Affairs* 80, no. 3 (2001): 98-112.
25. Associated Press. "China Boosts Information Warfare Development with Vast Research Centers." *Associated Press Worldstream*, September 27 2002.
26. Denning, Dorothy E. *Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy* Nautilus Institute, 1999 [cited March, 2003]. Accessed from http://www.terrorism.com.
27. Bolt, Paul J., and Carl Brenner. "Information Warfare across the Taiwan Strait." *Journal of Contemporary China* 13, no. 38 (2004): 129.
28. Drucker, Peter .F. *Managing in the Next Society (audiobook)*, *Audio Renaissance*. Los Angeles: St. Martin's Press/Truman Talley Books., 2002.
29. Toffler, Alvin. *The Third Wave*. New York: Bantam Books, 1981.
30. Meall, Lesley. "Survival of the Fittest." *Accountancy (UK)* 103, no. 1147 (1989): 140-41.
31. Critical Infrastructure Assurance Office. *Web Site* [cited May 1,, 2003]. Accessed from http://www.ciao.gov.
32. Garrick, John B., and Dana A. Powers. *Use of Defense in Depth In Risk-Information NMSS Activities (Letter to Richard A. Meserve dated May 25, 2000, Chairman, U.S. Nuclear Regulatory Commission)*, 2000 [cited June 17,, 2004]. Accessed from http://www.nrc.gov/reading-rm/doc-collections/acrs/letters/2000/4721893.html.
33. Wilson, Jim. "E-Bomb." *Popular Mechanics* 178, no. 9 (2001): 50-54.
34. Sunday Times. "Secret DTI Inquiry Into Cyber Terror." *The (London) Sunday Times*, June 9 1996, 1-8.
35. Stoll, Cliff. *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage*. New York: Doubleday, 1989.
36. Try a Google search on Home Depot, Texaco, or Wal-Mart for a demonstration.
37. Callamari, Peter, and Derek Reveron. "China's Use of Perception Management." *International Journal of Intelligence & Counter Intelligence* 16, no. 1 (2003): 1-15.
38. deCaro, Chuck. "Operationalizing SOFTWAR." In *Cyberware 2.0: Myths, Mysteries, and Reality*, edited by A.D. Campen and D.H. Dearth. Fairfax, VA: AFCEA International Press, 1998.
39. Cohen, William. *Former Defense Secretary Cohen's Remarks at the 2001 Summit (March 6)* George Mason University, 2001 [cited June 12, 2003]. Accessed from http://www.gmu.edu/departments/law/////techcenter/programs/summit/cohen's_2001_remarks.html.
40. Rosenoer, Jonathan. "Safeguarding Your Critical Business Information." *Harvard Business Review* 80, no. 2 (2002): 20-21.

41. Federal News Service. "Press Conference With Attorney General John Ashcroft; FBI Director Robert Mueller; and FTC Chairman Timothy J. Muris." *Federal News Service Inc.*, May 16, 2003.
42. Legard, David. *Fake Bank Web Site Scam Reaches U.S.* May 14, 2003 [cited June 12, 2003]. Accessed from http://www.itworld.com/Tech/2987/030514fakebank.
43. Ascribe. "Millennium Project Calls for Declaration of Global Information Warfare Against Transnational Organized Crime; Corruption, Money Laundering, Terrorism Funding by Organized Crime Should Be Treated as National Security Threat." *Ascribe Newswire*, February 10 2003.
44. Kolodzinski, Oscar. "Cyber-Insurance Issues: Managing Risk By Tying Network Security To Business Goals." *CPA Journal.* 72, no. 11 (2002): 10-11.
45. Keating, G. "Hacker Insurance Market Boosted by Cyberattacks." *Reuters*, January 27 2003.
46. Geralds, John. *Hacker Insurance Set to Rocket* February 14, 2003 [cited June 21,, 2004]. Accessed from http://www.vnunet.com/news/1138789.
47. Garg, Ashish, Jeffrey Curtis, and Hilary Halper. "The Financial Impact of IT Security Breaches: What Do Investors Think?" *Information Systems Security* 12, no. 1 (2003): 22-34.
48. Gross, G. "Net Attacks Down But Sophistication Is Up." *IDG News Service*, January 30 2003.
49. Straub, Detmar W. Jr., and Richard J. Welke. "Coping With Systems Risk: Security Planning Models for Management Decision Making." *Management Information Systems Journal* 22, no. 4 (1998): 441-69.
50. Dutta, Amitava, and Kevin McCrohan. "Management's Role in Information Security in a Cyber Economy." *California Management Review* 45, no. 1 (2002): 67-87.
51. International Information Systems Security Certification Consortium $(ISC)^2$. *Press Releases* Oct 31, 2002 [cited June 12, 2003]. Accessed from https://www.isc2.org/cgi/content.cgi?page=13.
52. Straub, Detmar W. Jr. "Effective IS Security: An Empirical Study." *Information Systems Research* 1, no. 3 (1990): 255-76.
53. Tucker, T. E. "Leveraging Protection Mechanisms to Provide Defense in Depth." In *Management of Information Security*, edited by M. E. & Mattord H. J. Whitman, 408. Boston: Course Technology, 2004.
54. Panko, Raymond. *Corporate Computer and Network Security*. New Jersey: Prentice Hall, 2004.
55. Austin, R. D., and C. A. R Darby. "The Myth of Secure Computing." *Harvard Business Review* 81, no. 6 (2003): 120-26.
56. Wood, Charles Cresson. *Information Security Policies Made Easy*. 5th ed: Baseline Software, 1996.